Chapter 2
Organizing for Improved Security
Jeff Recor

Computer and Network Security in Higher Education
Mark Luker and Rodney Petersen, Editors

A Publication of EDUCAUSE
Imagine you just started a new job as a newspaper carrier. You are not familiar with the route, the customers, or the rigors of the job. As you receive your allotment of papers on your first day, your boss says to you, “Make sure these papers are all delivered every morning by 10:00 A.M. no matter how bad the weather gets or how sick you become.” With little experience delivering papers and even less information about your customers, you take off to deliver your papers and find your way as you go. You have faith in your abilities and trust that you can work out any problems as they arise.

This allegory depicts the way many IT departments within academia have treated information security. Information security has typically been something to be added later. Worse yet, it is an area that has languished within information technology departments for years as the responsibility of overburdened system administrators or general IT staffers.

In the private sector, organizing for improved security typically is associated with establishing a formal information protection program (IPP). Steps that are taken by private sector organizations to establish a formal IPP include the following:

- Develop a single point of leadership responsible for the security function.
• Develop a support organization that is focused solely on security functions.

• Develop a security plan of action.

• Obtain operational, political, and financial support for the implementation of the plan of action.

Due to the open nature of academic environments and the protection of freedoms for the pursuit of knowledge, many higher learning institutions do not conform to the same practices that the private sector utilizes to organize for security. Fortunately, more and more academic institutions are recognizing the inherent risks associated with increased reliance on the use of information technology. As stated in the *National Strategy to Secure Cyberspace*, institutions of higher learning are starting to recognize the need to protect their resources and are examining ways to implement security functions that enable them to support their operations efficiently and affordably (*National Strategy*, 2003, pp. 40–41).

Formalizing a security-focused function within an academic environment is challenging because of the need to balance convenience (free and easy access to information) and openness (the ability to exchange ideas and information in a free and open environment) with security (the freedom from risk or danger). However, recent legislative, legal, competitive, and student pressures have forced academic institutions to rethink their approaches to handling information security. Colleges and universities are developing new security-focused roles and organizations within IT and other departments to support the mission of the institution. The old tactic of scaring people to act through fear, uncertainty, and doubt is being replaced with arguments supporting improved security and individual empowerment that does not compromise freedom of expression.
Establishment of a Security Infrastructure

All academic institutions can benefit from establishing an organized security infrastructure. This infrastructure comprises people, processes, and technology that can be directed toward securing the institutions’ assets within an open campus environment. It is no longer acceptable to put policies and procedures in place without some type of security hierarchy to support them.

The security support function can be dispersed among the many different departments on campus, or it can be centralized under a single entity such as information technology. Several factors can influence the way in which the security function is organized within an academic institution, such as

- Support of executive-level management and trustees
- Support of internal staff
- Requirements of external business partnerships (hospitals, military, private sector, and so forth)
- Politics within the institution
- Size of the institution
- Leadership and cooperation of IT and financial management teams

Each of these items can have a direct impact on the applicability of a formalized information security function.

Regardless of the method used to organize for improved security, institutions need to take action to protect their systems, people, and processes. Each year more security incidents occur that could have been prevented if the institution had taken action and properly incorporated information security functions into its day-to-day operations. Examples include the incident of a University of Delaware
student who was able to successfully hijack the passwords of several professors and change her grades (Read, 2002), and the incidents that caused federal officials to issue an alert regarding the security of college networks (Foster, 2002).

Institutions need to focus on the following critical functions when organizing to improve security:

- Developing a security plan of action that can be shared
- Obtaining support for the implementation of the plan of action
- Developing a mechanism for measuring progress of the security function
- Formulating partnerships and alliances to enhance internal capabilities
- Establishing security leadership
- Hiring or developing security expertise on staff

Developing a Security Plan of Action

The first step to organizing for improved security is to establish a security plan. The security plan will help the organization design its security strategy for supporting the operations of the institution. It will also formally define the items that need to be protected, the value they hold to the institution, the leadership structure needed to proactively manage the process, and many other operational details that will provide protection for the campus environment. The security plan will act as the overall security process blueprint, much as the security policies and procedures guide employee behaviors.

Obtaining Support for the Plan

Support from all levels of the institution is critical to a successful implementation. In general it is easier to obtain support for the plan
if its constructs have been developed and can be discussed among senior management. Communication of the plan, its reason for being, and its potential costs and benefits need to be clearly and concisely articulated to upper management in order to gain support.

The idea that information security is someone else’s problem is quickly disappearing. According to Michael McRobbie, vice president for information technology at Indiana University, “Colleges have a well-deserved reputation for lax network security. As a result, they risk increased insurance costs and expensive lawsuits” (Olsen, 2002, p. A35). However, in this environment of increased risk, many organizations still do not believe they need to worry about information security. So how do you sell upper management on the fact that they need to take information security seriously?

1. **Show them that information security adds value to the institution.** Although securing a campus environment takes time and money, it is a task that ultimately will protect staff, students, and partners, while also mitigating exposure to lawsuits, intellectual property loss, and employee problems.

2. **Match security needs to operational functions.** Gaining upper management support will take more than explaining the bits and bytes of the technology involved in protecting the institution. Strategy needs to be put into plain English and designed to support the goals of the institution.

3. **Establish frequent and concise reporting mechanisms to show improvement based on your actions.** For many managers, not hearing that anything bad has happened lulls them into a false sense of security. Often when security mechanisms are working properly, nothing will happen. Make sure management understands that no news is good news—especially if you can communicate that message regularly.

4. **Include security issues early in budgeting and IT planning processes.** Too often security technology is added “after the fact” and is
not integrated into a project from the beginning. By getting involved early, management may see the value that planning for security can have across the entire spectrum of project management.

The plan will also need the support of the department heads within the institution, as well as internal IT staff. To achieve this level of cooperation, academic institutions will sometimes establish committees consisting of representatives from different departments and use them as a “sounding board” for tweaking the plan’s goals and objectives.

**Measuring Progress**

Part of the process of organizing for improved security is to be able to learn from mistakes. Establishing a feedback loop through regular surveys will assist all personnel associated with the security function to learn how to better support the changing security environment. By monitoring numbers and types of security incidents, IT staff can track trends and develop more effective incident response strategies.

It is also important to monitor community satisfaction and awareness. Are faculty, students, and department staff pleased with the support they receive from the security program? Are there improvements that could be made? Asking these types of questions will enable communication to flow back and forth between the personnel performing security functions and their constituents.

**Forming Partnerships and Alliances**

Many different types of programs are being developed to help form bridges between private and public sector organizations. One commonly seen partnership of this type involves outsourcing central IT support. This has been done successfully at many institutions, with the goal of having better end-user support, lower costs, and improved service delivery.
Outsourcing the security function to a third party is a viable option for institutions that do not have the ability to handle security events internally. Of course there are pros and cons for such an arrangement, as with any outsourcing relationship. The benefits to the institution of outsourcing security include gaining the experience of security “experts,” having flexibility in meeting budget constraints, and obtaining a reduction in costs associated with maintaining the security function in-house. Among the downsides of such a relationship, the institution does not develop any in-house expertise and there is the potential for costs to increase. It is important to note that in any case, the responsibility and accountability for securing campus systems still rest with information technology leadership.

A new era of partnership is developing among employers, IT vendors, training organizations, and the public sector, fueled in many cases by the shortage of capable security professionals in today’s workforce. Institutions are considering all types of ways to leverage the private sector to increase its internal security expertise, as well as its capability to deliver educational services securely. Several institutions use their security teams as internal consultants who will charge for time according to use of their services. Still other institutions have been crafting agreements with companies such as Cisco, Microsoft, Hewlett-Packard, and Symantec to exchange security expertise and information on a contractual basis (www.cerias.purdue.edu/news_and_events/news/view_story.php?id=75). All of these types of arrangements help ensure that the institution’s security program accomplishes its goals and stays current with the latest trends.

Establishing Security Leadership

Critical to organizing for improved security is establishing dedicated leadership and skill sets. During the previous year, one of the most popular topics for discussion at security conferences and workshops involved the establishment of a security leadership role and skills
to support the function. Ideally, a dedicated security team would be led by an experienced professional who would provide expertise for developing and recommending policies and procedures, assessing vulnerabilities, detecting intrusions, responding to incidents, and developing an awareness program. However, many college and university environments do not support the creation of a single leadership position responsible for information security functions.

Many private-sector organizations are starting to support the addition of a new executive-level title called the chief security officer (CSO). Management consulting firm Booz Allen Hamilton in January 2002 surveyed firms with more than $1 billion dollars in annual revenues and found that 54 percent of the seventy-two chief executive officers it surveyed have a chief security officer in place. Ninety percent have been in that position for more than two years. When there is no chief security officer in place, chief information officers are more likely than other executives to have security responsibilities, the survey found (http://cin.earthweb.com/news/article.php/10493_997701). This position is similar to that of the chief information officer but is limited in scope to information security responsibilities.

Because security cuts across every line of business and every strategic decision, more and more companies are adding this position to their executive team. Typically, the CSO will report to a senior functional executive, such as a chief operating officer, chief administration officer, or head of legal counsel, and will coordinate security efforts across organizational units, including information technology, human resources, communications, legal, and facilities management.

Although this type of executive-level position is starting to gain momentum in the private sector, it does not appear to be catching on with colleges and universities. One of the main issues with establishing a leadership role for the information security responsibility is where this position obtains its executive-level support. Many CSOs currently report to the chief information officer and have to learn how to navigate through the IT political landscape.
in order to support other business units. Several very large organizations have recently started to move the reporting structure of the CSO to the chief executive officer. Within academic environments, appointing a single person with security leadership responsibilities can be a difficult task because of cultural, political, and organizational challenges. The size of the institution can also provide unique challenges to organizing security functions through a centralized leadership role. In the private sector, the role of chief security officer is often a shared function with the police office or public safety team.

**Hiring and Developing Security Expertise**

Providing leadership for information security functions is an important undertaking. In addition to choosing a leader for the security function, a team of individuals should also be considered to support the function. Several recent studies have shown security staffing levels to be erratic and unorganized. As a typical example of the proportion of security staff to information technology staff, a recent study by Computer Economics ranks IT security staffing levels by size of company (see Table 2.1). Another staffing survey, performed by *Information Security* magazine, shows the same type of information relating to the size of security teams (see Figure 2.1).

One of the items that these types of surveys highlight is the challenge that organizations face when trying to find staff with dedicated security skill sets. Because creating dedicated security teams is a relatively new endeavor for dealing effectively with security challenges, further studies need to be done to show how companies are handling security staffing issues.

**Basic Security Functions**

Another way to view security staffing is through the analysis of roles and responsibilities. A basic set of security functions should be established regardless of the size of the institution. Every institution
that utilizes computer technology has common functions that require some level of security functionality to protect information assets. These functions can be separated into three distinct areas: physical security, business operations security, and business continuity.

Physical Security

Physical security responsibilities can include locking up sensitive resources and information, monitoring the facilities, and using guards and alarms. For most institutions, these physical security tasks are designed and managed by a group that is separate from the IT organization. With the advent of new software and hardware that can join digital and physical monitoring, the management of physical security can be rolled into the traditional IT hierarchy or

Table 2.1. IT Security Staffing Levels.

<table>
<thead>
<tr>
<th>Number of Employees</th>
<th>Percentage of Organizations</th>
<th>Number of Security Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 25</td>
<td>13.8</td>
<td>48.2</td>
</tr>
<tr>
<td>26 to 50</td>
<td>9.1</td>
<td>81.9</td>
</tr>
<tr>
<td>51 to 100</td>
<td>0.0</td>
<td>56.2</td>
</tr>
<tr>
<td>101 to 250</td>
<td>14.3</td>
<td>42.8</td>
</tr>
<tr>
<td>251 to 500</td>
<td>0.0</td>
<td>26.7</td>
</tr>
<tr>
<td>501 to 1,000</td>
<td>15.4</td>
<td>46.2</td>
</tr>
<tr>
<td>1,001 to 2,000</td>
<td>7.1</td>
<td>7.1</td>
</tr>
<tr>
<td>2,001 to 5,000</td>
<td>12.5</td>
<td>6.2</td>
</tr>
<tr>
<td>5,001 to 10,000</td>
<td>0.0</td>
<td>7.1</td>
</tr>
<tr>
<td>Over 10,000</td>
<td>0.0</td>
<td>5.8</td>
</tr>
<tr>
<td>All organizations</td>
<td>7.0</td>
<td>29.6</td>
</tr>
</tbody>
</table>

Operational Security

Operational security functions include all of the traditional security responsibilities, such as placing firewalls to protect connections to the Internet, using access control management techniques, and auditing access controls and internal processes. Traditional security skills have been built around this core set of functionality, which includes firewall, intrusion detection, antivirus, and other product integration skill sets.

Business Continuity

The final category of common security functions is business continuity. Business continuity responsibilities include activities that provide the institution with the ability to continue operations in the
event of a disaster or other catastrophic event. Other activities that may fall into this category include data backup, load balancing, disaster recovery, and performance monitoring.

Security Professionals Assigned to Function

Based on these common functions, many institutions hire staff to manage day-to-day operations based on their needs in these three areas. Some of the more common job titles and their responsibilities are discussed next.

Security Administrator

The security administrator provides all technical administrative support for the IT organization, including performing liaison functions for other departments that may need support. The security administrator is responsible for maintaining security technology and reviewing log files for malicious activity.

Security Analyst

The security analyst assists the IT and information security staff with ensuring that all applicable business and policy requirements are met with the correct control functions and processes. The security analyst is often charged with reviewing the applicability of new technology and processes to see whether the organization can benefit from their use. In some instances, the security analyst may work with auditors or outside consulting organizations to perform risk assessments and review business continuity.

Security Engineer

The security engineer is a consultant in technical systems management who is the focal point and leader for design and implementation of security technology that supports the business objectives of the organization. People in this position work with various depart-
ments to ensure that the information security technology is
designed, installed, and maintained to function correctly.

Certification of Security Professionals

When hiring dedicated security personnel, most institutions are
concerned about both skills and salary. As market demand has
increased, professionals with security expertise have been in short
supply, and salaries have risen. Individuals with industry certifi-
cations are of particular interest; they bring defined sets of skills and
experience to the table, and consequently may expect higher com-
ensation. Certifications can cover everything from learning a com-
mon body of knowledge to focusing on a specific technology.
Although professional certifications do not guarantee a successful
hire or good organizational fit, they do provide the hiring institu-
tion with some assurance that the individual has basic competence
in the topics covered by the program. Some of the more popular cer-
tifications include the following:

- **Certified information systems security professional (CISSP)**. Created and maintained by the International Information Systems
  Security Certification Consortium, the CISSP requires four years of
  security-related experience plus the passing of a six-hour exam.
  Candidates are expected to master a common body of knowledge
  and adhere to professional ethics while certified (www.isc2.org).

- **Global information assurance certification (GIAC)**. The
  SANS (System Administration, Audit, Network, Security) Insti-
tute rolled out the GIAC in 1999 to address the need for specific
  technology mastery. The GIAC framework provides assurances
  that the candidates have mastered specific areas of technology,
  such as firewalls, intrusion detection, and incident handling
  (www.sans.org).

- **Security +**. The Computing Technology Industry Association
  (CompTIA) has developed an international benchmark certification
for security practitioners that measures foundational knowledge. This certification is considered to be a starting point for practitioners starting out in the field (www.comptia.org).

_Certification Magazine_ recently published a survey of the top security-related certifications as well as expected salary ranges of professionals with these certifications (www.certmag.com/articles/templates/cmag_sg.asp?articleid=71&zoneid=74.) The bottom line is that most surveys show that personnel with security certifications command salaries anywhere between $50,000 and $100,000 in the marketplace today.

**Use of Consultants**

An alternative to hiring dedicated security staff is to engage the services of an outside consulting organization. Institutions may use the services of an outside firm from time to time as a “check and balance” to measuring internal progress and effectiveness. Although outside security experts can help augment staff roles, hiring them is an expensive way to handle security functions day to day. Computer Economics, as part of the study referenced earlier, also took a look at the practices of organizations hiring outside consultants, as reflected in Table 2.2. This table shows that the institutions that use consultants the most are those that have a heavy emphasis on issues of legal or regulatory compliance.

**Conclusion**

The campus environment is constantly changing. Information security is a process that is also dynamic and becoming more important in the day-to-day operations of the institution. Just like the experienced newspaper carrier mentioned at the beginning of the chapter, once the route is defined the job is simply nothing more than focusing on delivering the papers. By organizing to improve security, institutions can improve their security posture and help protect our nation’s critical infrastructure.
Table 2.2. Organizations Contracting with a Security Consulting Firm During 2002.

<table>
<thead>
<tr>
<th>Industry Sector</th>
<th>Percentage of Respondents</th>
<th>Percentage of Respondents Who Have Contracted with a Security Consulting Firm During 2002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking, finance and insurance</td>
<td>14.6</td>
<td>27.9</td>
</tr>
<tr>
<td>Education</td>
<td>6.6</td>
<td>4.9</td>
</tr>
<tr>
<td>Government</td>
<td>16.5</td>
<td>21.3</td>
</tr>
<tr>
<td>Health care</td>
<td>4.7</td>
<td>8.2</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>11.3</td>
<td>13.2</td>
</tr>
<tr>
<td>Professional services</td>
<td>33.5</td>
<td>14.8</td>
</tr>
<tr>
<td>Retail, wholesale distribution</td>
<td>6.1</td>
<td>8.2</td>
</tr>
<tr>
<td>Trade services</td>
<td>2.8</td>
<td>1.6</td>
</tr>
<tr>
<td>Transportation and utilities</td>
<td>3.8</td>
<td>0.0</td>
</tr>
<tr>
<td>Number of Employees</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Less than 25</td>
<td>17.9</td>
<td>9.8</td>
</tr>
<tr>
<td>26 to 50</td>
<td>5.2</td>
<td>4.9</td>
</tr>
<tr>
<td>51 to 100</td>
<td>9.0</td>
<td>3.3</td>
</tr>
<tr>
<td>101 to 250</td>
<td>8.5</td>
<td>3.3</td>
</tr>
<tr>
<td>251 to 500</td>
<td>7.5</td>
<td>6.6</td>
</tr>
<tr>
<td>501 to 1,000</td>
<td>6.6</td>
<td>9.8</td>
</tr>
<tr>
<td>1,001 to 2,000</td>
<td>7.5</td>
<td>8.2</td>
</tr>
<tr>
<td>2,001 to 5,000</td>
<td>9.9</td>
<td>9.8</td>
</tr>
<tr>
<td>5,001 to 10,000</td>
<td>8.0</td>
<td>13.1</td>
</tr>
<tr>
<td>Over 10,000</td>
<td>19.8</td>
<td>31.1</td>
</tr>
<tr>
<td>Annual Revenue</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Under $1,000,000</td>
<td>22.3</td>
<td>20.0</td>
</tr>
<tr>
<td>$1,000,001 to $5,000,000</td>
<td>10.2</td>
<td>9.1</td>
</tr>
<tr>
<td>$5,000,001 to $10,000,000</td>
<td>6.6</td>
<td>7.3</td>
</tr>
<tr>
<td>$10,000,001 to $20,000,000</td>
<td>11.7</td>
<td>7.3</td>
</tr>
<tr>
<td>$20,000,001 to $50,000,000</td>
<td>8.1</td>
<td>3.6</td>
</tr>
<tr>
<td>$50,000,001 to $100,000,000</td>
<td>9.1</td>
<td>5.5</td>
</tr>
<tr>
<td>$100,000,001 to $1 billion</td>
<td>10.7</td>
<td>14.5</td>
</tr>
<tr>
<td>Over $1 billion</td>
<td>21.3</td>
<td>32.7</td>
</tr>
</tbody>
</table>

References


